REMARKS/ARGUMENTS

Reconsideration of the application is respectfully requested. Claims 1-2, 4-29 were rejected under Section 103 as being obvious over Kunzinger in view of Gunter. This rejection is respectfully traversed.

Claim 1 has now been amended to clarify that the secure forwarding if the message is from the first computer to the second computer using a secure connection and that the secure message is sent by using the same secure connection. No new matter has been added. Support may, for example, be found in paragraphs 0073-0083 of the corresponding US 2006/0173968.

Kunzinger merely teaches the use of two tunnels. He explains that the security gateway 420 (intermediary computer) serves as a point of entry into the intranet (paragraph 0050) and that the security gateway retains the ability to provide of the type of services available in the environment of Fig. 3. These services include access control and network address translation that require content inspection. In other words, the gateway protects the intranet from undesirable communication from the open Internet by inspecting the content of incoming packets before the packets enter into the intranet. This requires the gateway (intermediate computer) to decrypt the incoming packet in order to be able to inspect

the content of the incoming packet. In other words, Kunzinger expressly teaches away from any modification that would not allow the intermediate computer to decrypt the incoming packet to inspect the content (which would happen if Kunzinger is modified to include Gunter's extended tunnel, as proposed by the Examiner).

Fig. 4 of Kunzinger clearly shows that a first tunnel extends between the first computer (client) and the intermediate computer (boundary device or gateway) and a second tunnel extends between the intermediate computer and a second computer (server). The first tunnel provides security through the Internet and the second tunnel provides security through an intranet (see paragraph [0051] of Kunzinger). Kunzinger explains in paragraph [0047] that the "use of cascaded tunnels (as opposed to one tunnel or SA extending from the client to the server) allows security protection to be tailored to the requirements of a particular network segment."

Applicant fails to see why the skilled person would look to Gunter to modify Kunzinger to include a single tunnel extending from the client to the server when Kunzinger expressly teaches that such a modification should not be made because this would mean that the gateway would not be able to inspect the content of the incoming packets to protect the intranet from the outside public Internet.

In the current invention, the intermediate computer

does not need to know the cryptographic keys or read the content but is able to use the outer IP addresses and the incoming SPI value (= unique identity) to determine how to modify the outer address and the SPI to suite the second computer, which is the next destination.

In paragraph [0013], Kunzinger explains that the security associations are negotiated between the tunnel endpoints i.e. a first negotiation is between the endpoints of tunnel 1 and a second negotiation is between the endpoints of tunnel 2. This means the client 405 negotiates with the gateway 420 to establish tunnel 1 (but not with the server 440). Similarly, the gateway 420 negotiates with the server 440 to establish tunnel 2.

In summary, Kunzinger clearly teaches the use of cascade tunnels which provide the tailoring features (see paragraph [0047]) "as opposed to a tunnel or SA extending from the client to the server." In other words, he expressly teaches away from using a single tunnel from the client to the server. Also, in paragraphs [0012-0014] Kunzinger explains that each tunnel is a separate connection. In paragraphs 0067-0068 Kunzinger explains if there is no existing cascaded tunnel available between the gateway 420 and the server 440 then a pair of IKE and IPSsec security associations are established to provide the next tunnel (which again indicates that there are two separate tunnels and not one tunnel).

On page 5 of the Office action, the Examiner states

that Kunzinger teaches "the intermediate computer forwarding the secure message with the second destination address and the second unique identity to the second computer in the secure connection." (emphasis added). Applicant strongly disagrees. Kunzinger forwards the message in the second tunnel which is different from the first tunnel discussed on page 4 of the Office action. The current claim 1 requires that the message is sent in the same secure connection that extends from the first computer to the second computer.

On page 6, the Examiner states that it would have been obvious to combine the teachings of Kunzinger and Gunter to have endpoints directly negotiate a key to establish a secure connection. Applicant respectfully and strongly disagrees.

Kunzinger expressly states that the intermediate computer must be able to decrypt the message to protect the intranet (see paragraph 0050). If the secure connection is established by the endpoints of the tunnel, as suggested by Gunter, then the intermediate computer could not intervene and decrypt the message, as expressly required by Kunzinger. The Examiner is respectfully requested to better explain why the skilled person would modify Kunzinger to have one extended tunnel when Kunzinger expressly teaches away from this modification even if such an extended tunnel may be shown in Gunter.

Additionally, it is submitted that the secure tunnel

(Tunnel 1) in Fig. 3 could not extend between the client and the server because in Kunzinger, the gateways must have clear text access to datagrams as explained in paragraph [0027], lines 13-15. As indicated above, if the tunnel would be between the client and the server, then the gateway could not have clear text access to the datagrams. In paragraph [0017], Kunzinger explains that there are several disadvantages in providing an end-to-end security association between the two end-points (i.e. between the client and server, see paragraph 0017) because any "intermediate system in the network path are prevented from accessing the clear-text data content of the transmitted packets, because only the two endpoints are able to encrypt and decrypt the packets on this SA." In other words, Kunzinger expressly teaches away from a security association that extends between the client (first computer) and the server (the second computer) when the flag is set which is the only time the gateway would be using the id to identify the second computer. A secure connection that extends between the first computer and the second computer is exactly what is required by the amended claim 1 and that the intermediate computer uses the unique identity contained in the secure message to find the address to the second computer.

In order for the gateway (intermediate computer) of Kuntzinger to forward a packet it has to decrypt it (see paragraph 0068, lines 6-7. A key is needed for decryption which of course cannot be transmitted in the packet to be

decrypted. The key has been sent to the gateway in advance since a key is something used to encrypt and decrypt with (lock and unlock). A key is never sent in the same message as the encrypted message. It would be the same thing as leaving the key in a door when leaving your house.

There is a difference between encryption and hashing. Encryption transforms data from a cleartext to ciphertext and back (given the right keys), and the two texts should roughly correspond to each other in size: big cleartext yields big ciphertext, and so on. "Encryption" is a two-way operation. Hashes, on the other hand, compile a stream of data into a small digest (a summarized form: think "Reader's Digest"), and it is strictly a one way operation. A hash value is thus a unique and extremely compact numerical representation of a piece of data. Hashing is a one way function and a hash cannot be read by a receiver.

The Examiner states that "the key is the value id". It is respectfully submitted that this does not make sense. A key is a tool that is used to decrypt (remove encryption) from an encrypted message. If a key is sent together with an encrypted message, the encryption would be meaningless, since then anyone would have the key and be able to read the message. If again, the key would be sent as data in the encrypted message, the recipient could not take out the key from the message (being without a key to open the message). Thus, the key in Kunzinger is not an id and is not sent with

the message.

Gunter does not cure these deficiencies. Gunter is merely concerned with an ordinary key exchange (which is done to form a secure connection), but when the connection has been formed a device in an internal network send the keys to a firewall so that the fire wall could follow the connection. The forming of the connection takes place without the fire wall being present in the negotiation (see Fig. 4, reference numbers 200 and 202). The packets in the key exchange go through the firewall in the same way as through other routers (which are between the negotiating parties). The fire wall sends the packets to the internal network without decryption. This operation does not differ at all from ordinary router operation. The firewall of Gunter is able to decrypt the packets and store them but otherwise, it is just like an ordinary router.

Applicants fail to see why a person of ordinary skill in the art would look to Kunzinger and Gunter to learn about the steps of the present invention when Kunzinger expressly teaches away from this feature when the flag is set since Kunzinger's intermediate computer would be prevented from accessing the clear-text data content described in paragraph [0017]. When the flag is not set the gateway would not use any unique identity contained in the secure message to find an address for the second computer.

It is also noted that the Examiner has not commented

on all the arguments presented in the previous response. The Examiner is respectfully requested to review and consider all the arguments presented.

Also, paragraphs [0067] and [0068] of Kunzinger explain that the gateway decrypts that incoming data packet by using the decryption key that corresponds to the particular secure association i.e. Tunnel 1 extending between the client and the gateway. Kunzinger then explains that whether the message is intended to be forwarded further in the secured form (to the endpoint) then a Tunnel 2 has to be used and if there is no Tunnel 2 then it has to be established by means of a key exchange (IKE) procedure. Kunzinger explains that the policy "will direct the gateway to either use an existing cascaded tunnel, or if one is not available, to establish a pair of IKE and IPsec security associations that will provide this next cascaded tunnel. Kunzinger is here referring to Tunnel 2. This again confirms that Kunzinger requires two separate tunnels (secure connections) and it is submitted that it would not have been possible for Kunzinger's gateway to have decrypted the packet had the tunnel extended all the way between Kunzinger's client and server.

It is submitted that Kunzinger would require extensive modifications that are not taught or suggested to arrive at the features of the present invention. It is even submitted that Kunzinger would be inoperable by modifying it with Gunter's extended tunnel because Kunzinger's gateway

could not inspect the content of incoming packets.

In view thereof, claim 1 is submitted to be allowable.

Claims 2, 4-21 are submitted to be allowable because they depend upon the allowable base claim 1 and because each claim includes limitations that are not taught or suggested in the cited references.

Independent claim 22 is submitted to be allowable for reasons similar to the reasons put forth above. Claim 22 has been amended to now require that the secure message contains the unique identity and that the intermediate computer has a module performing the IPsec and IKE translation etc. without decrypting the secure message.

In contrast, the intermediate computer in Kunzinger decrypts the incoming secured message, as explained above. An important function of Kunzinger's gateways is to function as a port of entry into an intranet and to inspect the content of incoming secure packets which requires decryption of the packets before forwarding them to the server (the second computer) in the intranet. In other words, the decryption is an important function of Kunzinger's invention because the security gateway (intermediate computer) must be able to decrypt the packet so that it can provide the important services of access control, network address translation etc. that require content inspection, as explained in for example, paragraph [0050] of Kunzinger. Throughout the Kunzinger

patent, the feature of content inspection is emphasized and it is submitted it would be contrary to the spirit of Kunzinger to modify his system to prevent the security gateway from being able to inspect the content of the incoming packets. It is submitted that Kunzinger expressly teaches away from extending the tunnel from the client to the server so that the gateway could not decrypt the incoming packet. The proposed modification is therefore not obvious even if another reference such as Gunter shows a tunnel that has an intermediary computer that cannot decrypt the incoming packet.

Claims 23-26 are submitted to be allowable because they depend upon the allowable base claim 22 and because each claim includes limitations that are not taught or suggested in the cited references.

Independent claim 27 is submitted to be allowable for the same reasons as those put forth for the patentability of claim 22. In addition, the amended claim 27 requires a module for performing the IPsec and IKE translation etc. without undoing the IPsec processing and being aware of the keys to encrypt and/or authenticate the secure message and without establishing a new IPsec connection and that the secure message contains the unique identity. It is submitted that Kunzinger expressly teaches away from extending the tunnel from the client to the server so that the gateway could not decrypt the incoming packet. The proposed modification of Kunzinger is therefore not obvious.

Claims 28-29 are submitted to be allowable because they depend upon the allowable base claim 1 and because the claims include limitations that are not taught or suggested in the cited references.

Claim 3 was rejected under Section 103 as being obvious over Kunzinger in view of Patel. This rejection is respectfully traversed.

Claim 3 is submitted to be allowable because it depends upon the allowable base claim 1 and because the claim includes limitations that are not taught or suggested in the cited references.

The application is submitted to be in condition for allowance, and such action is respectfully requested.

Respectfully submitted,

FASTH LAW OFFICES

/rfasth/
Rolf Fasth
Registration No. 36,999

ATTORNEY DOCKET NO. 290.1078USN

FASTH LAW OFFICES
26 Pinecrest Plaza, Suite 2
Southern Pines, NC 28387-4301

Telephone: (910) 687-0001
Facsimile: (910) 295-2152